KEY SYNCHRONIZATION MECHANISM FOR WIRELESS LAN (WLAN)

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to wireless networks. More particularly, it relates to a synchronization mechanism for a wireless local area network (LAN).

2. Description of the prior art

A key challenge to successful deployment of Wireless LANs (WLAN) is securing the wireless link. Due to its wireless nature, hacking into or gaining access and snooping into the data contained on any other computer on the wireless network is fairly trivial in a WLAN. Thus, data must be encrypted to prevent such unauthorized viewing. This encryption can be done either at the application layer or at the link layer level. The link level encryption is more useful as it does not require any modifications to existing applications. There are several mechanisms available to secure WLANs at the link layer:

Wired Equivalent Privacy (WEP)

Although WEP is by far the most widely used method, it has been shown to have several weaknesses. One main weakness being the absence of automatic periodic renewal of the encryption key. Thus, if someone captures enough WEP encrypted packets, it becomes relatively easy to deduce the encryption key.

WiFi Protected Access (WPA)

WPA is a relatively new standard that overcomes some short comings of WEP. It provides a mechanism for key rotation and hence is more secure.

Since WEP is the most widely deployed mechanism, solutions that enable key rotation in the WEP have been proposed. However, this leads to the problem of encryption key synchronization. The WLAN Access Point (AP) and the wireless station (STA) must share the same WEP encryption key. During initial encryption key setup and key rotation, it is possible that the AP and the STA get out of sync, i.e., the AP and STA update their encryption keys at slightly different times and hence have different encryption keys. During this out-of-sync period, the AP and the STA will not be able to communicate with each other. Worse yet, because they are out of sync, the signaling protocol exchange between them for encryption key setting may not be able to finish, creating a deadlock.

This problem not only occurs in the proposed key rotation in the WEP solutions, but may also occur with any type of mechanism in which the data packets (frames) used in the signaling protocol for key setting are encrypted. The present invention proposes a

mechanism to solve the encryption key synchronization problem.

WPA does not suffer from the same problems as WEP key synchronization due to the fact that signaling protocol data is unencrypted. However, concerns have been raised regarding the unencrypted signaling data being explored by hackers. The proposed encryption key synchronization mechanism of the present invention can be used within the WPA framework with encrypted signaling data frames.

SUMMARY OF THE INVENTION

In accordance with an aspect of the invention, the encryption key synchronization method for wireless local area networks (WLAN) includes setting a current encryption key and an old encryption key at an access point in the WLAN and sending an encrypted data frame from a station in the WLAN to the access point using a first encryption key. Initially the old encryption key is set to an empty value (null). Decryption of the received data frame is performed by the access point using the current key (i.e., the current key at the AP is equal to the first key at the STA).

A new encryption key is generated at the access point upon expiration of a key refresh interval and sent to the station in an encrypted form using the first key. The access point resets the old key to be equal to the first key, and resets the current key to be equal to the newly generated key.

The access point receives a data frame and determines whether the encryption key being used by the station sending the data frame is the current key or the old key. This is determined by the access point by attempting to decrypt the data using the current key first. If that fails, the access point uses the old key to decrypt the data. If the key being used by the station is the old key and not the current key, the access point increments an out-of-sync counter indicating decryption failure since the station has not started using the newly generated key (i.e., current key).

When the access point determines that the data frame received from the station is using the new key, the access point starts using the new key and decrypts the data frame using the same. The access point then resets the old key to be equal to the current key, and resets the out-of-sync counter to zero showing that synchronization between the access point and station has been achieved using the new key.

Other objects and features of the present invention will become apparent from the following detailed description considered in conjunction with the accompanying drawings. It is to be understood, however, that the drawings are designed solely for purposes of illustration and not as a definition of the limits of the invention, for which reference should be made to the appended claims. It should be further understood that the drawings are not necessarily drawn to scale and that, unless otherwise indicated, they are merely intended to conceptually illustrate the structures and procedures described herein.

BRIEF DESCRIPTION OF THE DRAWINGS

In the drawings wherein like reference numerals denote similar components throughout the views:

Figure 1 is a block diagram of a WLAN according to an aspect of the invention; and

Figure 2 is a processing diagram of the key synchronization mechanism according to an aspect of the invention.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

The present invention is directed to a system/mechanism and method for encryption key synchronization for wireless LANs. Advantageously, the present invention allows for more secure encryption key synchronization in the key rotation used in WLAN data encryption. The key synchronization is performed at the link layer level. Accordingly, the present invention advantageously provides a more reliable encryption key synchronization mechanism that can be used at the link layer in WEP, WPA or other types of link layer mechanisms used to secure WLANs.

In accordance with an aspect of the invention, the access point (AP) maintains two encryption keys for each Station (STA). After a new key is set for the communication session between an AP and an STA, the AP does not start using the new key until the first data frame correctly encrypted with this new key is received from the STA. This new key will be used for the session between the AP and the STA from that point on. The AP also maintains an out-of-sync counter that is used to track the number of packets that could not be decrypted because of mismatched encryption keys.

It is to be understood that the present invention may be implemented in various forms of hardware, software, firmware, special purpose processors, or a combination thereof. Preferably, the present invention is implemented as a combination of hardware and software. Moreover, the software is preferably implemented as an application program tangibly embodied on a program storage device. The application program may be uploaded to, and executed by, a machine comprising any suitable architecture. Preferably, the machine is implemented on a computer platform having hardware such as one or more central processing units (CPU), a random access memory (RAM), and input/output (I/O) interface(s). The computer platform also includes an operating system and microinstruction code. The various processes and functions described herein may either be part of the microinstruction code or part of the application program (or a combination thereof) that is executed via the operating system. In addition, various other peripheral devices may be connected to the computer platform such as an additional data storage device and a printing device.

It is to be further understood that, because some of the constituent system components and method steps depicted in the accompanying Figures are preferably implemented in software, the actual connections between the system components (or the process steps) may differ depending upon the manner in which the present invention is programmed. Given the teachings herein, one of ordinary skill in the art will be able to contemplate these and similar implementations or configurations of the present invention.

Referring to Figure 1, there is shown a WLAN 100 having a plurality of stations STA1, STA2, ...STA_N, 120, 122, ...124, respectively, and at least one access point (AP) 110. In other contemplated systems, there may be additional access points AP 112.

Figure 2 shows the key synchronization process 200 between an access point 110 and a station 120 according to an aspect of the invention. By way of example, two encrypt and decrypt processes 206 and 216 are shown. For purposes of this description, the term "station key" refers the encryption key being used by the station. As shown in the example of Figure 2, the station key is initially K1 (204), and upon expiration of the key refresh interval, the station key will be K2. In addition, the terms "encryption key" and "key" are interchangeable throughout this description.

On key rotation, the AP 110 maintains and saves the last used key Kold and the new key Kcurrent (202). For exemplary purposes, it is assumed that both the AP and STA are initially in sync. In other words both share the same encryption key and are able to securely communicate with each other. As shown, K1 is set (204) at the STA, and Kcurrent = K1 (202) at the AP. The AP also initially sets Kold to a null value, as no new keys are generated until the expiration of the first key refresh time interval after starup. The STA sends an encrypted packet (208) using key K1, and the AP decrypts the packet (210) using the Kcurrent = K1 key with success.

At step 212, or the expiration of a key refresh interval (key rotation interval), the AP generates new key K2, sets Kold = K1 and Kcurrent = K2. The AP sends key K2 (214) to the STA after it is generated and while the previous link using key K1 is still in tact. Thus, key K2 is sent to the STA 120 in an encrypted state.

An out-of-sync condition arises when the AP has started using key K2 while the STA is still using key K1. In other words, all of the packets being sent from the STA (218) to the AP are encrypted with station key K1. The AP attempts to decrypt the packets with Kcurrent (i.e., key K2) and hence fails (220). The AP can make this determination by checking the CRC checksum at the end of each frame. Every time the AP fails to decrypt a packet, it increments an out-of-sync counter Csync by 1 (222). The out-of-sync counter Csync is used to track the number of packets that could not be decrypted because of mismatched encryption keys. Since the AP could not decrypt the packet with Kcurrent it re-tries to decrypt it with Kold (224). Since Kold is set to K1, the decryption is successful. Thus, the first indication to the AP 110 that a new key is being used by the STA 120 is determined when the first packet successfully encrypted using the new key that has been received and decrypted by the AP 110.,

In a short time the STA also updates its key and starts using K2 (226) as its station key. The STA will then send (228) an encrypted packet using key K2. The AP is now able to decrypt the packets using Kcurrent (230). As soon as the AP receives the first correctly encrypted packet, it resets Csync=0, and sets Kold = Kcurrent (230). This process ensures that a malicious user who was able to deduce key K1 is unable to access the AP at the expiration of the key refresh period.

The out-of-sync counter Csync is maintained to ensure that the STA does not remain out-of-sync for long. Once Csync exceeds a pre-defined threshold, the STA is de-authenticated. This action will thwart a malicious user who may have been able to deduce key K1.

Those of skill in the art will recognize that in the above description, any of the keys could be null, which corresponds to no encryption. For example, at the initial key setting (202), there may not be any encryption, Kold is thus null. The above mechanism works the same way. This is because the AP not only can tell whether a frame is correctly encrypted with a particular key, it can also tell whether a frame is encrypted or not.

While there have been shown, described and pointed out fundamental novel features of the invention as applied to preferred embodiments thereof, it will be understood that various omissions, substitutions and changes in the form and details of the methods described and devices illustrated, and in their operation, may be made by those skilled in the art without departing from the spirit of the invention. For example, it is expressly intended that all combinations of those elements and/or method steps which perform substantially the same function in substantially the same way to achieve the same results are within the scope of the invention. Moreover, it should be recognized that structures and/or elements and/or method steps shown and/or described in connection with any disclosed form or embodiment of the invention may be incorporated in any other disclosed, described or suggested form or embodiment as a general matter of design choice. It is the intention, therefore, to be limited only as indicated by the scope of the claims appended hereto.